Universidad de Santiago
Facultad de Ciencias
Departamento de Matemática y Ciencia de la Computación

Introducción a la Criptografía Moderna
Laboratorio 2

Prof: Rodrigo Abarzúa

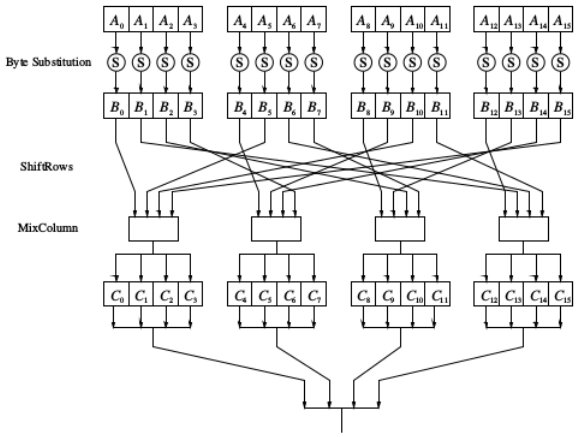
April 3, 2017

1 AES: Advanced Encryption Standard

En 1997 NIST llamo a concurso para proponer el nuevo Advanced Encryption Standard (AES).
La selección del algoritmo para AES fue un proceso público administrado por NIST. En tres rondas de evaluación NIST y la comunidad científica internacional discutió las ventajas y desventajas de los cifradores sometidos en el concurso. En el 2001, NIST declaro que el cifrador de bloques Rijndael es el nuevo AES y publicó el estándar final FIPS PUB 197. Rijndael fue diseñado por los criptógrafos Belgas Joan Daemen y Vincent Rijmen ambos estudiantes de la Katholieke Universiteit Leuven.
Los requisitos que debía cumplir este nuevo criptosistema eran: Cifrado de bloque, con bloques de 128-bits. Debía soportar claves de longitud: 128, 192 y 256 bit. Eficiente en software como en hardware.

1.1 AES

En la siguiente figura, se presentan de manera Global el funcionamiento del AES



1.2 Byte Substitution Layer

- La primera capa de cada ronda es el **Byte Substitution Layer** .
- Esta capa se puede ver como 16 filas en paralelo aplicadas en S-Boxes cada una con entradas y salidas de 8 bits. Se debe notar que todos los 16 S-Boxes son idénticos a diferencia de DES cuando se utilizan ocho diferentes S-Boxes.
- En esta capa, cada estado de byte A_i es sustituido por otro byte B_i : $S(A_i) = B_i$.
- La lookup tabla de todas los $S(A_i) = B_i$ se puede ver en la siguiente figura.

									y							
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
x 8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

- Se debe observar que el elemento cero no tiene inverso. Sin embargo, para el AES se define el elemento $A_i = 0$ es llevado a si mismo.

1.3 Capa de difusión

- En el AES, la capa de difusión consiste de dos subcapas:
  - La transformación **ShiftRows** y la transformación **MixColumn**.
  - Recordemos que la difusión es la propagación de la influencia de los bits individuales sobre todo el estado.

1.3.1 ShiftRows Sublayer:

- La transformación **ShiftRows** es un shifts cíclico Tabla 1, por ejemplo:
- Supongamos que la entrada a la subcapa del **ShiftRows** es dada por la matriz $B = (B_0, B_1, \ldots, B_{15})$

B_0	B_4	B_8	B_{12}	$\leftarrow$ no shift
B_5	B_9	B_{13}	B_1	$\leftarrow$ una posición de shift izquierda
B_{10}	B_{14}	B_2	B_6	$\leftarrow$ dos posiciones de shift izquierda
B_{15}	B_3	B_7	B_{11}	$\leftarrow$ tres posiciones de shift izquierda

Table 1: ShiftRows.

1.3.2 Column Sublayer:

- La transformación MixColumn es lineal y mezcla cada columna de la matriz de estado.
- La idea es que cada byte de entrada tiene influencia en los cuatros bytes de salida.
- La transformación MixColumn es la operación que entrega mayor difusión en el AES.
- La combinación de ShiftRows y MixColumn hace posible que después de tres rondas cada byte de la matriz de estado depende de todos los 16 bytes del plaintex.
- Denotemos el 16-byte del estado de entrada B y los 16-byte de estado de salida $C : MixColumn(B) = C$, donde B es el estado después de la transformación ShiftRows.
- Ahora, cada columna de 4-byte se considera como una vector y multiplicado por una matriz fija de 4×4.
- La matriz contiene entradas contantes. La multiplicación y adiciones es realizada en $GF(2^8)$, por ejemplo:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

- Más detalladamente la multiplicación entre el vector y la matriz en esta operación se realiza en $GF(2^8)$ donde cada byte C_i y B_i es un valor de $8-$bit en $GF(2^8)$.
- Los coeficientes de la matriz en notación hexadecimal se utiliza, es decir:
  - 01 se refiere al polinomio con coeficientes (00000001) en $GF(2^8)$ es decir es el elemento 1 en este cuerpo.
  - 02 es el polinomio (00000010) es decir el polinomio x en $GF(2^8)$.
  - 03 se refiere al polinomio con bit (00000011) es decir es el polinomio $x + 1$ de $GF(2^8)$.

2 Laboratorio:

Considere el problema de implementar la función del AES.

2.1 Se solicita:

1. Implementar una ronda de la función AES. Dados las variables explicadas anteriores.
2. Implementar en lenguaje C un algoritmo para la función AES.
3. Se debe entregar:

- Código fuente del algoritmo.
- Informe en LaTeX que contiene:
  - Algoritmo implementado.
  - Formulación del experimento.
  - Curvas de desempeño de resultados.
  - Conclusiones.